## *Amendments to the Claims*

1 – 23. (canceled)

24. (previously presented) A cryptographic accelerator for performing an RC4 stream cipher, comprising:

a multi-ported memory having at least three read ports and at least two write ports; and

a cryptographic core having a four-stage pipeline, wherein during a key generation process the cryptographic core is configured to:

in a first stage, increment the value of a first memory address location,

in a second stage, read data stored at a previous first memory address location and calculate a value of a second memory address location,

in a third stage, read data stored at a previous second memory address location, calculate a value of a third memory address location, and write data stored at a previous first memory address location to the previous second memory address location, and

in a fourth stage, read data stored at a previous third memory address location and write data stored at the previous second memory address location to a previous first memory address location,

wherein after three initialization clock cycles, a byte of a key stream is generated in the fourth stage by the cryptographic core in each subsequent clock cycle.

25. (previously presented) The cryptographic accelerator of claim 24, wherein during the three initialization clock cycles, the cryptographic core is configured to:

in a first cycle, increment the first memory address location to a first i value in the first stage;

in a second cycle, increment the first memory address location to a second i value in the first stage, read data stored at the first memory address location having the first i value and calculate a first j value for the second memory address location in the second stage; and

in a third cycle, increment the first memory address location to a third i value in the first stage, read data stored at the first memory address location having the second i value and calculate a second j value for the second memory address location in the second stage, and in the third stage, read data stored at the second memory address location having the first j value, calculate a first t value for the third memory address location, and write data stored at the first memory address location having the first i value into the second memory address location having the first j value.

26. (previously presented) The cryptography accelerator of claim 25, wherein in subsequent cycles the cryptographic core is configured to:

in the first stage, increment the first memory address location to an $n^{th}$ i value,

in the second stage, read data stored at the first memory address location having the $(n-1)^{th}$ i value and calculate an $m^{th}$ j value for the second memory address location,

in the third stage, read data stored at the second memory address location having the $(m-1)^{th}$ j value, calculate an $r^{th}$ t value for the third memory address

location, and the write data stored at the first memory address location having the (n-2)$^{th}$ i value into the second memory address location having the (m-1)$^{th}$ j value; and

in the fourth stage, read data stored at the third memory address location having the r$^{th}$ t value and output the read data as the keystream byte and write the data stored at the second memory address location having (m-2)$^{th}$ j value into the first memory address having the (n-2)$^{th}$ i value.

27. (previously presented) The cryptography accelerator of claim 26, wherein if the (n-1)$^{th}$ i value used in the read operation of the second stage is the same as the (m-1)$^{th}$ j value used in the write operation of the third stage, then the cryptographic core acquires data for the read operation of the second stage from an input line to the multi-ported memory.

28. (previously presented) The cryptography accelerator of claim 26, wherein if the (m-1)$^{th}$ j value used in the write operation of the third stage is the same as the (n-2)$^{th}$ i value used in the write operation of the fourth stage, then write operation of the fourth stage is not performed by the cryptographic core.

29. (previously presented) The cryptography accelerator of claim 24, wherein the multi-ported memory is a register.

30. (previously presented) The cryptography accelerator of claim 29, wherein the multi-ported memory is a flip-flop based register.

31. (previously presented) The cryptography accelerator of claim 24, wherein the cryptographic core is further configured to shuffle the values stored in the memory addresses of the multi-ported memory, including:

in a first stage, increment the value of a first memory address location,

in a second stage, read a value stored at a previous first memory address location and calculate a second memory address location;

in a third stage, read data stored at a previous second memory address location and write the data stored at a previous first memory address location to the previous second memory address location, and

in a fourth stage, write the data stored at the previous second memory address location to a previous first memory address location.